Information Security Risk Assessment

**Document instructions:** Make a copy of this file and then fill it out.

# Introduction

A security assessment will be performed on all IT Resources to ensure a balance of risk, threats, vulnerabilities, and countermeasures to achieve an acceptable level of risk associated with the classification of the IT resource.

## 1.1 Purpose

The purpose of this assessment is to establish the system and data classification of the IT resource, to identify threats and vulnerabilities, and to provide a list of risks identified that could adversely affect our organization’s risk posture.

## 1.2 Scope

This assessment will identify the risks with the following IT Resource: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 1.3 Participants

| **Role** | **Participants** |
| --- | --- |
| IT Asset Owner |  |
| IT Asset Custodian |  |
| Risk Assessment Team |  |

# Risk Assessment Approach

## 2.1 Techniques Used

The Techniques used in this assessment will include a data and system classification questionnaire, the risk model, an external 3rd party vulnerability assessment tool and worksheets to identify threats, vulnerabilities and risks.

## 2.2 Risk Model Definitions and Formula

**Risk** is evaluated based on the probable **likelihood** and probable **severity** of a *threat* acting upon a *vulnerability* causing harm to an IT Resource.

**Threat** is defined as a circumstance or event with the potential to cause an adverse impact on the organization.

**Vulnerability** is an inherit weakness in a system.

**IT Resource**  - IT Asset, system, application, group of systems or process

**Sensitivity** – In our model this is an IT Resource’s tolerance for risk

**Risk Exposure = Sensitivity x Severity x Likelihood**

## 2.3 Risk Model Scales

Figure 2.3a Sensitivity Scale

| **Sensitivity Scale Risk Tolerance of the IT Resource** | |
| --- | --- |
| Critical  (5) | A compromise to this resource would be unacceptable for the organization. Result in harm to life or property, significant monetary penalties and fines, loss of productivity or reputational losses.  Business operations would be shut down or significantly impaired. |
| High  (4) | A compromise to this resource would be unacceptable for the organization. Result in significant monetary, productivity or reputational losses. Business operations would be greatly impaired. |
| Moderate (3) | A compromise to this resource would be marginally acceptable for the organization. Result in some monetary, productivity, or reputational losses. Business Operations would be noticeably impaired. |
| Low  (2) | A compromise to this resource would be limited, acceptable for the organization. Minimal monetary, productivity, and reputational losses. Minimal impact to normal business operations. |

Figure 2.3b Severity Scale

| **Severity (Impact) Scale**  **The impact if a threat event occurs** | |
| --- | --- |
| Critical  (5) | A threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, or other organizations. |
| High  (4) | A threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, or other organizations. |
| Moderate (3) | A threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other or organization. |
| Low  (2) | A threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals or other organizations. |

Figure 2.3c Likelihood Scale

| **Likelihood Scale The probability of a threat exploiting a vulnerability** | |
| --- | --- |
| Very High (5) | A threat event caused by error, accident, act of nature, or malicious adversary is **almost certain** to occur. Very little or no security controls are in place and vulnerabilities are exploitable from the internet. |
| High  (4) | A threat event caused by error, accident, act of nature, or malicious adversary is **highly likely to occur.**  Security controls are ineffective and threat source is highly motivated and capable. |
| Moderate (3) | A threat event caused by error, accident, or act of nature or malicious adversary is **somewhat likely** to occur. Security controls in place to impede successful exploit and threat source is only partially motivated and capable. |
| Low  (2) | A threat event caused by error, accident, act of nature or malicious adversary is **not likely to occur**. Security controls in place will prevent or significant impede successful exploit. |

# 3. IT Resource Profiling and Data Classification

3.1 Resource Profiling Questionnaire

Figure 3.1a Resource Sensitivity

| **Resource Profiling Questions** | **Please fill in the blank or check the box as applicable.** | |
| --- | --- | --- |
| Who uses this resource?  (Ex: Employees, Partners/Vendors, Departments, other)? |  | |
| Described the data this resource contains. Is any of the data stored on this resource sensitive?  (Ex: Credit card info, Social Security numbers, personal identifiable information, sensitive corporate) |  | |
| Rate the impact of corruption or unauthorized modification/destruction of data on this resource. (Loss of Integrity) | ☐ Low  ☐ Moderate | ☐ High  ☐ Critical |
| Rate the impact of unauthorized disclosure or compromise of the data on this resource. (Loss of Confidentiality) | ☐ Low  ☐ Moderate | ☐ High  ☐ Critical |
| Rate the impact of loss or disruption of services of this resource. (Loss of Availability) | ☐ Low  ☐ Moderate | ☐ High  ☐ Critical |
| What would be the legal ramifications if this resource were breached or unavailable? | ☐ Low  ☐ Moderate | ☐ High  ☐ Critical |
| What would be the reputational consequences if this resource were breached or unavailable? | ☐ Low  ☐ Moderate | ☐ High  ☐ Critical |
| Would there be regulatory consequences if this resource were breached or unavailable? | ☐ Low  ☐ Moderate | ☐ High  ☐ Critical |
| What would be the financial consequences if this resource were breached or unavailable? | ☐ Low  ☐ Moderate | ☐ High  ☐ Critical |

## 3.2 Data Classification

Figure 3.2a Data Classification

| **Based on the Data Classification definitions below, please check the data classification of this resource.** | |
| --- | --- |
| **☐ Class A Critical** | Information that must be available for the organization to effectively perform its mission and meet its legal obligations, and for which special precautions are taken to ensure its accuracy, relevance, timeliness, and completeness. This information, if unavailable, could cause significant financial loss, potentially pose a hazard to life and or health, or delay in performance of the organization's mission and or meeting its legal obligations. |
| **☐ Class A Restricted** | Information that has either mandatory or discretionary limitations placed upon both its access within and disclosure outside the organization in accordance with a court order, applicable law, Federal statute or mandate, or organization policy. |
| **☐ Class B Controlled** | Information that management has determined to require limitations or internal access/distribution on a need to know basis; does not include restricted information. |
| **☐ Class B Limited Controlled** | Information that can be readily made available to the public. |

## 3.3 System Classification

Figure 3.3a System Classification

| **Based on the System Classification definitions below, please check the system classification** | |
| --- | --- |
| **☐ Class A Critical Systems** | A computer system that requires protection because the process is critical to the operation of the organization, that is, if adversely manipulated or not run on or near schedule will cause significant financial loss to the company, pose a hazard to life and or health or delay in performance of the organization's mission and or meeting its legal obligations. |
| **☐ Class A Restricted Systems** | A computer system that requires protection because the information or process is classified as restricted, that is, has limitations placed upon both its internal access and external exposure. |
| **☐ Class B Controlled** | A computer system that management has determined requires specific protection mechanisms or access limitation placed upon both its internal access and external exposure. |
| **☐ Class B Limited Controlled** | A computer system that requires minimal protection and limitations placed upon its internal and external access and disclosure. |

## 3.4 IT Resource Sensitivity Rating

Based on the answers given above, please rate the Risk Sensitivity of this IT Resource. This is its tolerance to risk.

| **Risk Sensitivity Score** | ☐ Low | ☐Moderate | ☐High | ☐Critical |
| --- | --- | --- | --- | --- |

\*See Figure 2.3a Sensitivity Scale

# 4 Security Risk Analysis

In this section, we will begin to identify threats and vulnerabilities to this resource in order to calculate risks.

## 4.1 System Information

Figure 4.1a System Information

| **Please answer the questions in the space below regarding the system information of this IT Resource:** | |
| --- | --- |
| Describe the category of your resource. It could be a System, Group of systems, infrastructure, application, database or a process. |  |
| What System(s) is this IT Resource installed on? And what OS are the system(s) installed on? |  |
| Are the OS patches up-to-date? |  |
| Are the Vendor patches up-to-date? |  |
| Are patches done on a recurring basis for this resource? |  |

## 4.2 Information Flow

Figure 4.2a Information Flow

| **Please answer the questions in the space below regarding the way information flows in regards to this IT Resource:** | |
| --- | --- |
| Does the IT resource sit in the internal network or DMZ? |  |
| Is this Resource publicly accessible from the Internet? |  |
| Briefly describe the way information flows with this IT Resource. |  |
| What security controls do you already have in place to keep this resource secured? |  |

## 4.3 Threat and Vulnerability Identification

A threat source is the source of an exploit. A threat event is the exploit that can occur when a vulnerability is present. A vulnerability is a lack of a countermeasure or a weakness in a countermeasure that is in place. Hardware, software, procedures or people can all be weaknesses that can be exploited.

The following table below gives examples of possible threat sources, threat events and vulnerabilities.

| **Threat Sources** | **Threat Events** | **Vulnerabilities** |
| --- | --- | --- |
| Natural Disaster  Environmental failures  Infrastructure failures  Malicious insider  Malicious outsider  Accidental insider  External targeted attacker  Operational Processes | Phishing and Spear phishing attacks  DOS and DDOS  Accessing and Disclosure of sensitive data  Zero Day exploits  Propagation of malware and Trojans  Session Hijacking  Modification or destruction of sensitive data  Natural disasters and environmental failure | Cross-Site Scripting  SQL injection  Poor Software coding  Sensitive Data Exposure  Authentication weaknesses  Buffer overflows  Vendor vulnerabilities  Software vulnerabilities  Weakness in a process/lack of countermeasure |

## 4.4 Identification of Risks

List the threat/vulnerability pairs and the likely impact of the threat event occurring. Then rank the Severity of impact and the likelihood of occurrence. The numerical values are listed in the tables below. Sensitivity will be a static value defined in Resource Profiling Section.

| **Severity and Likelihood Scores**  **\*See scales on page 3** | Low=2 | Moderate=3 | High=4 | Critical=5 |
| --- | --- | --- | --- | --- |

To determine Risk Exposure, multiply the numerical values of Sensitivity, Severity and likelihood. Use the table below to determine the Risk Exposure Level.

| **Risk Exposure Scoring**  **Total value of Sensitivity x Severity x Likelihood** | Low = 1-16 | Moderate = 17-39 | High = 40-73 | Critical=+74 |
| --- | --- | --- | --- | --- |

**Sensitivity x Severity x Likelihood = Risk Exposure**

|  | **Threat Source/**  **Threat Event** | **Vulnerability** | **Impact** | **Sensitivity** | **Severity** | **Likelihood** | **Risk**  **Exposure** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Example:  Distributed Denial of Service (DDoS) attack. | Lack of controls to detect | Severely hinder the organization to conduct business | High  4 x | Critical  5 x | Moderate  3 = | High  60 |
| 2 |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |